Keamanan Jaringan Komputer

Scanning and Mapping CVE

Oleh :

M. Sulkhan Nurfatih

09121001061

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2016

Scanning and Mapping CVE

Pada MID mata kuliah keamanan jaringan komputer kami diberi tugas untuk melakukan scanning sebuah web dengan menggunakan tools yang sudah ditentukan sebelumya. Berikut ini adalah tools yang digunakan dalam melakukan scanning :

1. Zenmap
2. Nessus
3. Netcut

Scanning yang dilakukan adalah :

1. Scanning Open Port
2. Scanning Deamon (Service)
3. Scanning Vulnerability
4. Mapping CVE dari Deamon

Namun, disini kita akan membagi tugas dari tools yang tersedia untuk melakukan scanning. Berikut ini pembagian tugas dari tools scanning :

1. Zenmap

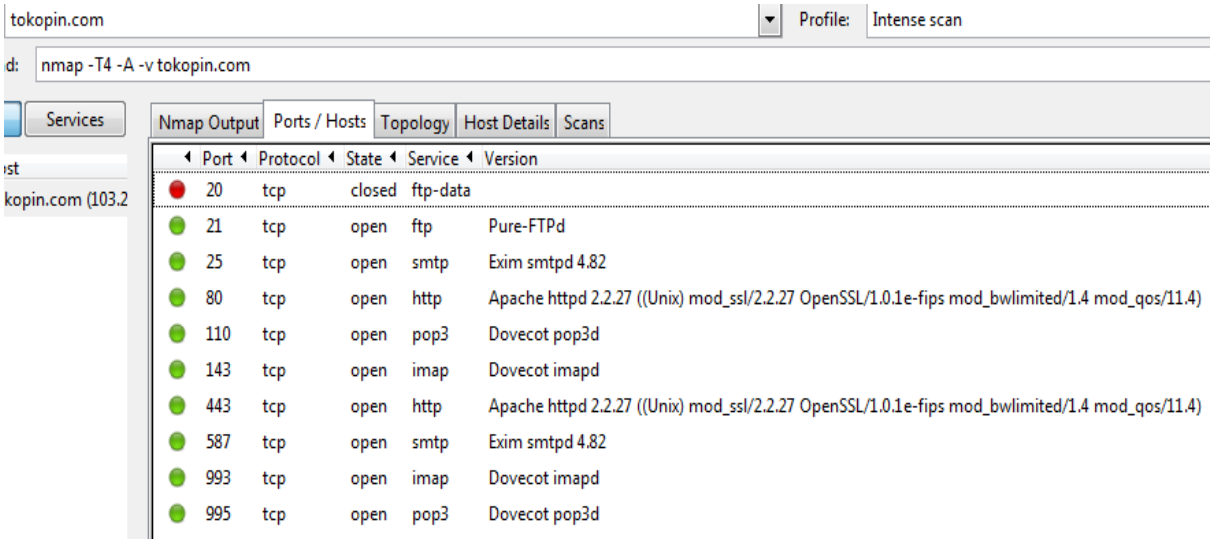
   Nmap akan kita gunakan untuk scanning Open Port dan Deamon. Karena, pada saat menggunakan zenmap kita tidak dapat mengakses untuk mengetahui vulnerability. Sehingga kita akan gunakan untuk mengetahui open port dan deamon (service)/
2. Nessus

   Nessus akan kita gunakan untuk scanning Vulnerability. Karena, tools ini sangat support untuk melakukan scanning tersebut.
3. Netcut

   Netcut akan kita gunakan untuk scanning Open Port saja. Namun, sistem yang digunakan adalah mengecek satu per satu port yang sudah di scanning oleh zenmap sebelumnya. Bisa dibilang kita melakukan coba-coba pada port default yang kita sudah tahu pada umumnya.

Scanning yang dilakukan menggunakan OS Windows dan Linux. Dimana, dalam menjalankan nmap dan nessus kita menggunakan OS Windows. Sedangkan, untuk menjalankan netcut kita menggunakan OS Linux. Target scanning disini adalah web yang beralamatkan www.tokopin.com dengan IP address 103.29.215.195.

a. Zenmap



Gambar 1.1 Tampilan hasil scanning open port dan deamon (service)

b. Nessus

tokopin.com

Summary

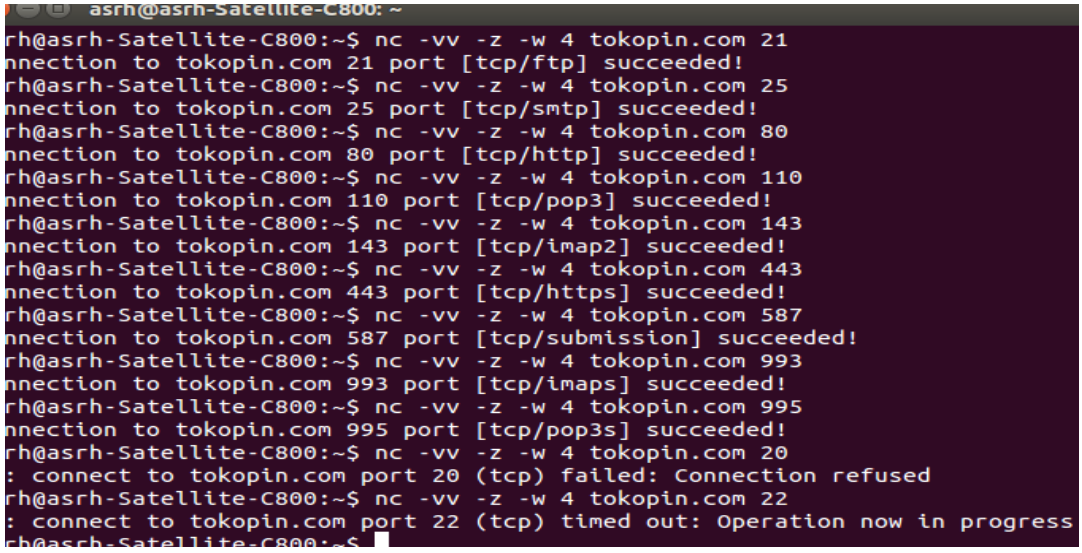
Critical	High	Medium	Low	Info	Total
0	0	12	5	39	56

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
Medium (5.0)	88098	Apache Server ETag Header Information Disclosure
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
Medium (4.3)	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
Low (2.6)	15855	POP3 Cleartext Logins Permitted
Low (2.6)	31705	SSL Anonymous Cipher Suites Supported
Low (2.6)	54582	SMTP Service Cleartext Login Permitted
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled

Gambar 1.2 Tampilan hasil scanning vulnerability

c. Netcut



Gambar 1.3 Tampilan hasil scanning open port

Selanjutnya kita akan menganalisis hasil scanning yang dilakukan dimulai dari open port, deamon, vulnerability, dan CVE yang ada pada deamon. Namun, sebelumnya kita akan membatasi berapa port yang akan kita analisis. Dalam hal ini kita akan menganalisis 3 port yang ada yaitu port 21, 25, dan 80. Ketiga port ini adalah salah satu port yang open / terbuka dari beberapa port yang terbuka pada web target.

a. Open Port

- Port 21

  Pada server target port 21 terbuka yang berarti server memiliki FTP (File Transfer Protokol) yang digunakan untuk berbagi file. Ketika seseorang mengakses FTP server, maka ftp client secata default akan melakukan koneksi melalui port 21.

- Port 25

  Pad server target port 25 terbuka yang berarti server memiliki SMTP (Simple Mail Transfer Protocol), atau port server mail yang merupakan port standar yang digunakan dalam berkomunikasi pengiriman e-mail antara sesama SMTP Server.

- Port 80

  Pada server target port 80 terbuka yang berarti server memiliki layanan web server, yang menyediakan informasi di dalam web tersebut. Port ini menggunakan protocol http sebagai media komunikasi user. Port ini adalah port yang paling umum digunakan di internet dan port yang merupakan standar yang digunakan dalam menjalankan web server.

b. Deamon (Service)

- Port 21

  Pada port 21 menggunakan deamon Pure-FTPd yang merupakan aplikasi ftp yang mengijinkan user yang mempunyai akses untuk mengupload file dan mendownload file. Pure-FTPD merupakan salah satu service yang banyak digunakan untuk proses upload dan download antara perangkat localhost (ftp client) dengan remote host (ftp server). Service Pure-FTPD ini memiliki banyak fitur diantaranya dari sisi keamanan, didukung oleh banyak system operasi, cukup banyak di terjemahkan dalam banyak bahasa untuk pesan servernya, memiliki fleksibilitas dan banyak diintegrasikan dengan layanan web hosting panel seperti cpanel atau lainnya untuk mendukung service layanan web hosting server.

- Port 25

  Pada port 25 menggunakan deamon Exim smtpd 4.82. Exim sendiri adalah sebuah aplikasi Mail Transfer Agent yang kembangkan untuk komputer-komputer berbasis Unix yang terkoneksi ke internet. Akan tetapi, untuk mengirimkan email dari linux kea kun email seperti (yahoo, gmail, dan sebagainya) kita membutuhkan smtp server sebagi relay. Kita dapat menggunakan smtp dari gmail sebagai relay email yang dikirim dari mesin linux ke inbox email kita.

- Port 80

  Pada port 80 menggunakan deamon Apache httpd 2.2.27. Apache sendiri merupakan server web yang dapat dijalan dibanyak sistem operasi seperti Unix, BSD, Linux, Windows, dan platform lainnya yang digunakan untuk melayani dan memfungsikan situs web. Protokol yang digunakan untuk melayani fasilitas web/www ini mengunakan HTTP. Apache memiliki fitur-fitur seperti pesan kesalahan yang dapat dikonfigur, autentikasi berbasis basis data dan lain-lain. Apache juga didukung oleh sejumlah antarmuka pengguna berbasis grafik (GUI) yang memungkinkan penanganan server menjadi mudah.

c. Vulnerability

- Port 21

  Pada port 21 zenmap tidak dapat menemukan versi dari deamon yang digunakan pada server. Sehingga kita tidak dapat menemukan vulnerability yang terdapat pada port 21 yang digunakan oleh server target.

- Port 25

  Pada port 25 zenmap berhasil menemukan versi dari deamon yang digunakan pada server yaitu Exim smtpd 4.82. Jika kita lihat dari CVE terdapat kelemahan pada versi ini yaitu Exec Code + Priv yaitu dimana execute code memungkinkan untuk penyerang mengeksekusi program yang seharusnya dia tidak diberi hak akses. Serta, untuk Priv disini adalah escalating privilage dimana dari user biasa dapat menjadi root tanpa atau menggunakan password.

- Port 80

  Pada port 80 zenmap berhasil menemukan versi dari deamon yang digunakan pada server yaitu Apache httpd 2.2.27. Jika kita lihat dari CVE terdapat kelemahan dari versi ini yaitu rentan terhadap serangan DoS. DoS merupakan jenis serangan terhadap sebuah komputer atau server didalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh sebuah komputer tersebut sampai komputer tersebut didapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

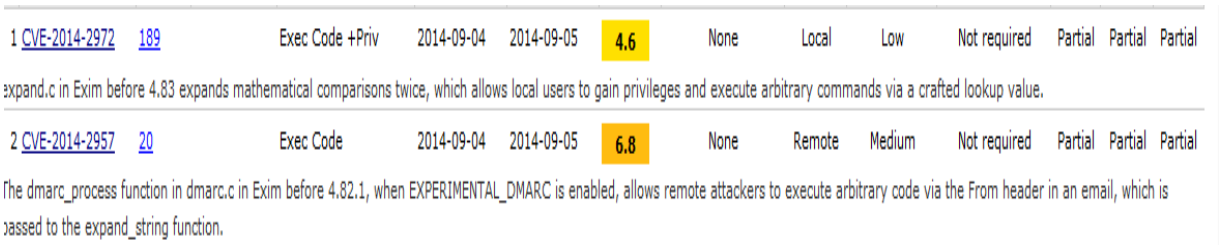
d. Mapping CVE dari Deamon

- Port 21

  Tidak berhasil menemukan CVE-nya karena zenmap tidak dapat menemukan versi dari deamon Pure-FTPd.

- Port 25

  Ditemukan CVE pada port 25 dengan deamon Exim smtpd 4.82 berikut tampilannya :



Gambar 1.4 Tampilan CVE port 25

Pada gambar 1.4 dapat kita lihat terdapat dua CVE yaitu CVE-2014-2972 dan CVE-2014-2957. CVE ini adalah CVE yang ada pada deamon Exim smtpd 4.82. Untuk Mapping CVE kita membutuhkan informasi CVE versi sebelumnya sekitar 3 sampai 4 tahun sebelumya. Berikut ini adalah hasil scanning CVE dari Exim smtpd 4.70 sampai 4.82 :

Cpe Name:*cpe:/a:exim:exim:4.70*
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

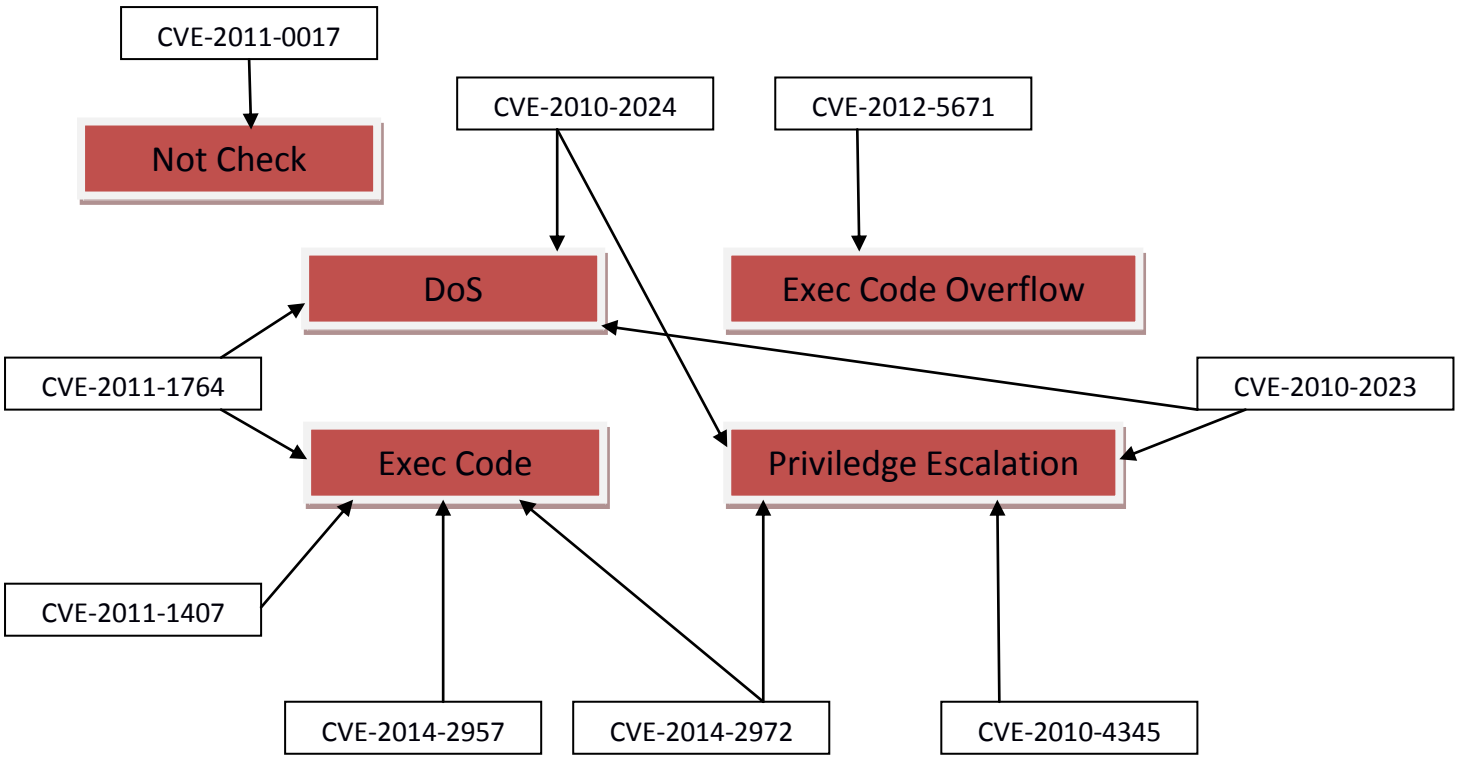
Copy Results Download Results Select Table

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2014-2972	189		Exec Code +Priv	2014-09-04	2014-09-05	4.6	None	Local	Low	Not required	Partial	Partial	Partial
expand.c in Exim before 4.83 expands mathematical comparisons twice, which allows local users to gain privileges and execute arbitrary commands via a crafted lookup value.														
2	CVE-2014-2957	20		Exec Code	2014-09-04	2014-09-05	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
The dmarc_process function in dmarc.c in Exim before 4.82.1, when EXPERIMENTAL_DMARC is enabled, allows remote attackers to execute arbitrary code via the From header in an email, which is passed to the expand_string function.														
3	CVE-2012-5671	119		Exec Code Overflow	2012-10-31	2013-04-18	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
Heap-based buffer overflow in the dkim_exim_query_dns_txt function in dkim.c in Exim 4.70 through 4.80, when DKIM support is enabled and acl_smtp_connect and acl_smtp_rcpt are not set to "warn control = dkim_disable_verify," allows remote attackers to execute arbitrary code via an email from a malicious DNS server.														
4	CVE-2011-1764	134		DoS Exec Code	2011-10-04	2014-02-20	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Format string vulnerability in the dkim_exim_verify_finish function in src/dkim.c in Exim before 4.76 might allow remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via format string specifiers in data used in DKIM logging, as demonstrated by an identity field containing a % (percent) character.														
5	CVE-2011-1407	20		Exec Code	2011-05-16	2011-09-06	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
The DKIM implementation in Exim 4.7x before 4.76 permits matching for DKIM identities to apply to lookup items, instead of only strings, which allows remote attackers to execute arbitrary code or access a filesystem via a crafted identity.														
6	CVE-2011-0017	59			2011-02-01	2011-03-01	6.9	None	Local	Medium	Not required	Complete	Complete	Complete
The open_log function in log.c in Exim 4.72 and earlier does not check the return value from (1) setuid or (2) setgid system calls, which allows local users to append log data to arbitrary files via a symlink attack.														
7	CVE-2010-4345	264	1	+Priv	2010-12-14	2011-02-17	6.9	None	Local	Medium	Not required	Complete	Complete	Complete
Exim 4.72 and earlier allows local users to gain privileges by leveraging the ability of the exim user account to specify an alternate configuration file with a directive that contains arbitrary commands, as demonstrated by the spool_directory directive.														
8	CVE-2010-2024	362		DoS +Priv	2010-06-07	2011-02-17	4.4	None	Local	Medium	Not required	Partial	Partial	Partial
transports/appendfile.c in Exim before 4.72, when MBX locking is enabled, allows local users to change permissions of arbitrary files or create arbitrary files, and cause a denial of service or possibly gain privileges, via a symlink attack on a lockfile in /tmp/.														
9	CVE-2010-2023	362		DoS +Priv	2010-06-07	2011-02-17	4.4	None	Local	Medium	Not required	Partial	Partial	Partial
transports/appendfile.c in Exim before 4.72, when a world-writable sticky-bit mail directory is used, does not verify the st_nlink field of mailbox files, which allows local users to cause a denial of service or possibly gain privileges by creating a hard link to another user's file.														

Total number of vulnerabilities : 9 Page : 1 (This Page)

Gambar 1.5 Tampilan scanning CVE dari tahun 2010 sampai 2014

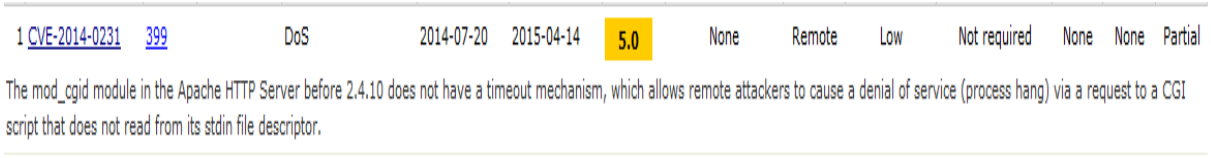
Berikut ini adalah gambaran mappingnya :



Gambar 1.6 Tampilan mapping CVE dari tahun 2010 sampai 2014

- Port 80

  Ditemukan CVE pada port 80 dengan deamon Apache httpd 2.2.27 berikut tampilannya :



1	CVE-2014-0231	399	DoS		2014-07-20	2015-04-14	5.0	None	Remote	Low	Not required	None	None	Partial

The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

Gambar 1.7 Tampilan CVE port 80

Pada gambar 1.7 dapat kita lihat terdapat dua CVE yaitu CVE-2014-0231. CVE ini adalah CVE yang ada pada deamon Apache httpd 2.2.27. Untuk Mapping CVE kita membutuhkan informasi CVE versi sebelumnya sekitar 3 sampai 4 tahun sebelumya. Berikut ini adalah hasil scanning CVE dari Apache 2.2.23 sampai 2.2.27 :

Cpe Name:*cpe:/a:apache:http_server:2.2.23*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

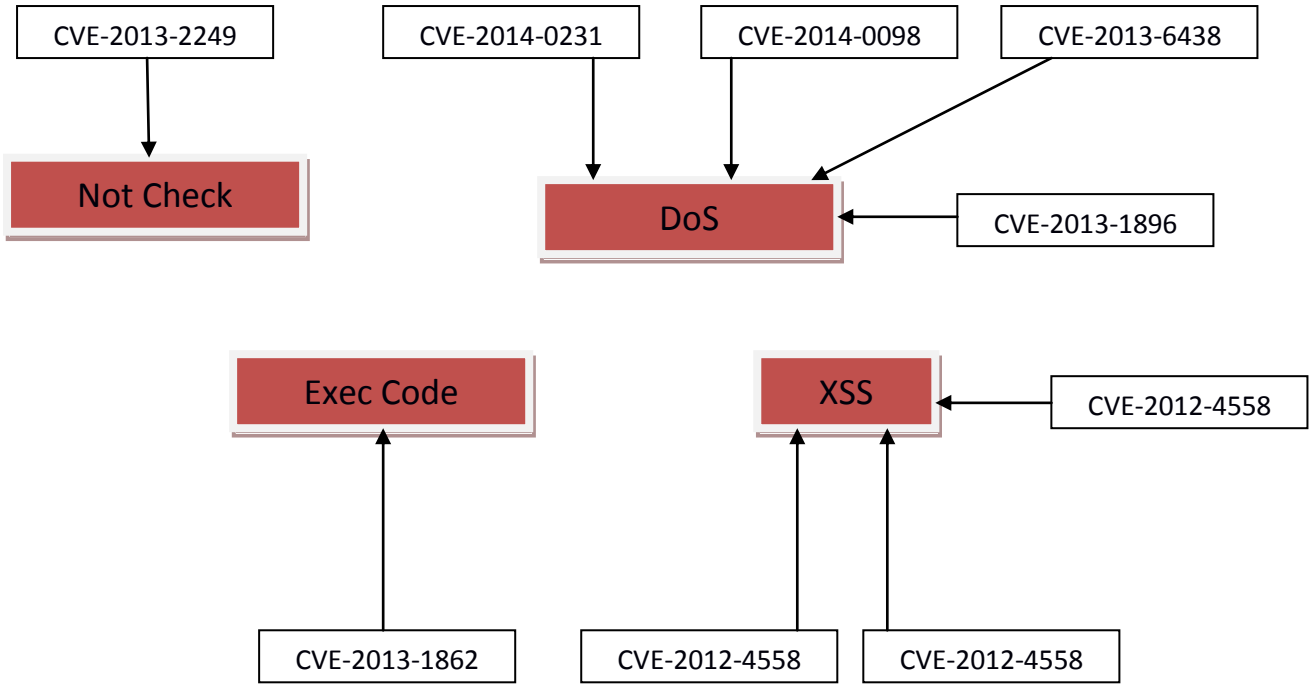
Copy Results Download Results Select Table

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2014-0231	399		DoS	2014-07-20	2015-04-14	5.0	None	Remote	Low	Not required	None	None	Partial
	The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.													
2	CVE-2014-0098	20		DoS	2014-03-18	2015-05-15	5.0	None	Remote	Low	Not required	None	None	Partial
	The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.													
3	CVE-2013-6438	20		DoS	2014-03-18	2015-05-15	5.0	None	Remote	Low	Not required	None	None	Partial
	The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.													
4	CVE-2013-2249				2013-07-23	2013-08-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
	mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.													
5	CVE-2013-1896	264		DoS	2013-07-10	2014-03-05	4.3	None	Remote	Medium	Not required	None	None	Partial
	mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI.													
6	CVE-2013-1862	310		Exec Code	2013-06-10	2014-03-05	5.1	None	Remote	High	Not required	Partial	Partial	Partial
	mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.													
7	CVE-2012-4558	79		XSS	2013-02-26	2014-01-17	4.3	None	Remote	Medium	Not required	None	Partial	None
	Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.													
8	CVE-2012-3499	79		XSS	2013-02-26	2014-01-17	4.3	None	Remote	Medium	Not required	None	Partial	None
	Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.													
9	CVE-2012-2687	79		XSS	2012-08-22	2013-12-05	2.6	None	Remote	High	Not required	None	Partial	None
	Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.													

Total number of vulnerabilities : **9** Page : 1 (This Page)

Gambar 1.8 Tampilan scanning CVE dari tahun 2012 sampai 2014

Berikut ini adalah gambaran mappingnya :



Gambar 1.9 Tampilan mapping CVE dari tahun 2012 sampai 2014

Daftar Pustaka

“Pure-FTPd” http://www.chrootid.com/instalasi-ftp-server-menggunakan-pureftpd/ (diakses 24 Maret 2016)

“Exim-4.82” https://www.cvedetails.com/vulnerability-list/vendor_id-10919/product_id-19563/version_id-170893/Exim-Exim-4.82.html (diakses 24 Maret 2016)

“Apache 2.2.27” https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-180675/Apache-Http-Server-2.2.27.html(diakses 24 Maret 2016)

http://www.jakethitam.com/2015/06/mengirim-email-dari-linux-dengan-exim4.html (diakses 24 Maret 2016)

“DoS” https://id.wikipedia.org/wiki/Serangan_DoS (diakses 24 Maret 2016)

“Apache” https://id.wikipedia.org/wiki/Apache_HTTP_Server (diakses 24 Maret 2016)